[19]中华人民共和国国家知识产权局

[51]Int.Cl[6]
H04N 7/16

[12]发明专利申请公开说明书

[21]申请号 98118377.8

[43]公开日 1999年2月24日

[11]公开号 CN 1209017A

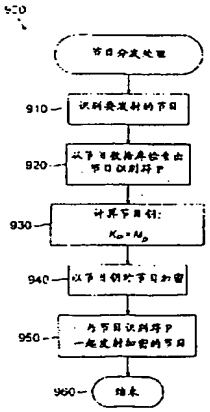
[22]申请日 98.8.14 [21]申请号 98118377.8
[30]优先权
[32]97.8.15 [33]US[31]912,186
[71]申请人 朗迅科技公司
地址 美国新泽西
[72]发明人 阿维沙·伍尔
[74]专利代理机构 中国国际贸易促进委员会专利商标事务所
代理人 鄭 迅

权利要求书5页 说明书15页 附图页数10页

[54]发明名称 用节目识别符限制访问发射的节目内容的加密方法和装置

[57]摘要

这里公开了一种用于限制对发射的节目内容进行访问的系统,该系统与加密的 节目内容一起发射一节目识别符。机顶终端或相似的机制应用存储的解密钥限 制对发射的多媒体信息的访问。机顶终端最好相应于在一给定期间授权给用户 一个或多个节目包,周期性地从头端接收权利信息。每个节目最好由头端服务 器在发射之前应用一个对该节目是唯一的节目钥 KP 来加密。机顶终端应用接 收到的节目识别符 p,与存储的权利信息一起,导出对该节目解密所必需的解密 钥。



目可以在200,000这个数量级。

在一个变化中，常规的机顶终端包含一个位向量，该位向量具有相应于由服务提供者提供的节目包的一位入口。一般，每一节目包相应于一个电视频道。如果特定用户被授权到一节目包，则将存储在机顶终端中的位向量中的相应位入口设置为一(“1”)。此后，由服务提供者发射的所有节目以一单个密钥加密。在接收到一给定节目后，机顶终端访问该位向量，以确定是否已设置相应位入口。如果该位入口已被设置，机顶终端就应用一单个存储的解密钥对节目解密。

在理论上，通过为每一节目提供一个位入口在位向量方案中达到灵活性时，在一单个计费期间发射许多节目的系统中位向量的长度是不切实际的。另外，在这样一个系统中的访问控制是由位向量中的入口唯一提供的，而且不是加密的。于是，如果用户能够重写该位向量，并设置所有的位为一(“1”)，则用户能访问所有节目。

在进一步的变化中，节目被分成节目包，并且在一给定节目包中的所有节目以相同的密钥加密。每一节目包一般还是相应于一个电视频道。机顶终端为授权给用户的每一节目包存储一个解密钥。于是，如果一个节目要包含在多个节目包中，则该节目必须为每一相联系的节目包重新发射，每次发射以相应于特定节目包的加密钥加密。虽然访问控制是加密的，多次发射一给定节目的额外开销使得服务提供者不愿意将同一节目放在多个节目包中，从而限制了在节目包设计中的灵活性。

虽然这些用于加密和发射节目内容的前述系统已经比较成功地限制了已授权用户的访问，但这些系统不允许服务提供者，例如电视网络，向用户提供包含各种数目的节目的许多不同的节目包，而不超过机顶终端的有限的保密存储器容量或显著地增加额外开销。由于用于发射加密节目内容的常规系统存在着上述明显缺陷，因此需要有一种系统，用于发射带有节目识别符并以密钥加密的节目，该节目识别符由机顶终端使用，与存储的权利信息一起，导出对节目解密所必需的解密钥。还需要一种系统，该系统允许服务提供者在多个节目包中包括某个节目，而不需要服务提供者为每一节目包重新发射该节目。还需要一种访问控制系统，该系统克服了机顶终端的保密存储器限制，而不会显著地增加与发射的节目内容相联系的

额外开销。

通常，服务提供者应用一发射器或者头端服务器向一个或多个用户发射加密节目内容。依据本发明的一个方面，将用于识别节目的节目识别符 p 与节目内容一起发送给用户。每一用户最好具有一机顶终端或另一机制，以应用解密钥来限制对发送的多媒体信息的访问。机顶终端最好相应于在一给定期间授权给用户的一个或多个节目包，周期性地接收来自头端的权利信息。

每一节目最好由头端服务器在发射之前应用一个节目钥 KP 加密，其中节目钥 KP 对该节目可以是唯一的。除了发射加密的节目，头端服务器最好还向机顶终端发射节目识别符 p 。机顶终端应用接收到的节目识别符 p，与存储的权利信息一起，导出对该节目解码所必需的解码钥。以这种方式，如果一特定节目授权给用户，则机顶终端应用存储的和接收的信息可以导出加密节目钥 KP，并在此后应用该节目钥 KP 对加密的节目解密。在各种实施例中，该节目识别符 p 可以与节目部分交叉或者在一个单独专用的控制频道上发射。

依据本发明的另一方面，每一个用于对发射的节目加密的 k-位节目钥 KP 是若干 k-位主密钥集 m1...mn 所定义集合的线性组合，每一主密钥 mi 最好由头端服务器存储在一个 k × n 矩阵 M 的列中。节目钥 KP 的位长度 k 必须比节目识别符 p 的位长度 n 大。节目识别符 p 作为一节目密钥掩码，指定在主密钥矩阵 M 中的哪一个密钥被用于产生节目钥 KP 。头端服务器最好在每一计费期间为矩阵 M 产生一个新的主密钥集。在一个实施例中，主密钥矩阵 M 可以随机产生，假设主密钥 mi 是线性无关的，以使得产生的节目钥 KP 不会意外地为 0 。

用户购买一个或多个所需的节目包，这些节目包一起包含了 r 个节目。因为每一用于对节目加密的节目钥 KP 是主密钥集 M 的线性组合，所以一旦用户获得了授权的 r 个节目的每一个的节目钥 KP，则用户也可以很容易地导出 2r 个节目的节目钥 KP 。于是，依据本发明的另一方面，需要 r 个节目的用户实际获得对包含这些 r 个节目的节目的最小线性子空间 U 的访问。最好以一种允许带有相关内容的节目符合低维线性子空间的方式来组织节目。另外，因为每一节目钥 KP 是主密钥 M 的线性组合，所以一给定

节目包不能具有任意数目的节目。特别地，一个节目包包括(2i-1)个节目识别符，对 i 小于 n 的某些值，这些节目识别符不必都指定给节目。

机顶终端需要对任何属于用户的授权子空间 U 内的节目 p 解密，但不对任何其他节目解密。子空间 U 可以用一个基矩阵 B 来表示。为了对分别由一节目识别符 p 识别的节目的子空间 U 解密，机顶终端需要一个从主密钥矩阵 M 导出的主密钥的相应子集。于是，机顶终端包括一个用户密钥矩阵 K，该矩阵包含授权给用户的主密钥的导出部分。另外，由机顶终端存储的权利信息包括一个有效行下标集 i1...ir，该有效行下标集由头端服务器用来从基矩阵 B 和正则基矩阵的逆矩阵(B()-1 生成一正则矩阵 B(。

在一个最佳实施例中，机顶终端还存储一个校验矩阵 C，作为权利信息的一部分，以允许机顶终端提前确定接收的节目是否在授权子空间 U 中，而不用经过整个解密过程。以这种方式，机顶终端可以明确地将因为发射错误而无法解密的节目与因为不是子空间 U 的成员而无法解密的节目区分开来。

通过参考下面的详细说明和附图，可以更全面地理解本发明，以及本发明的其他特征和优点。

图 1 是显示依据本发明的一个实施例用于发送加密节目内容的系统的方框图;

图 2 是图 1 中的头端服务器例子的方框图;

图 3 是图 1 中的机顶终端例子的方框图;

图 4a 和 4b 显示了一个用于获得由图 3 中的机顶终端存储的权利信息的线性方程系统;

图 5 显示了来自图 2 的节目数据库的样本表;

图 6 显示了由图 2 的头端服务器用于以一种允许带有相关内容的节目适合一低维线性子空间的方式组织节目的典型的主题分层结构;

图 7 显示了来自图 3 的权利数据库的样本表;

图 8a 是说明由图 2 的头端服务器实现的权利信息分发处理的例子的流程图;

图 8b 显示了由图 8a 的权利信息分发处理为图 6 中的具有一 m-位前缀掩码的主题计算出的基向量集 B(;

说 明 书 附 图

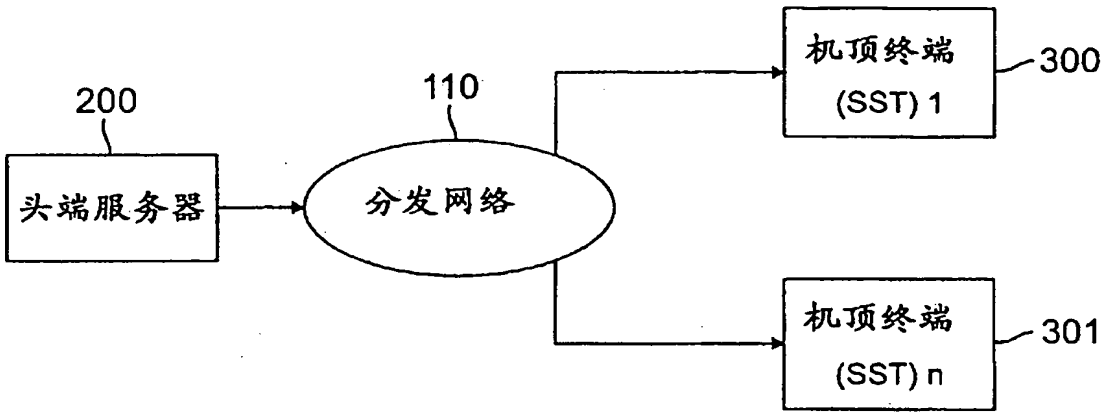


图 1

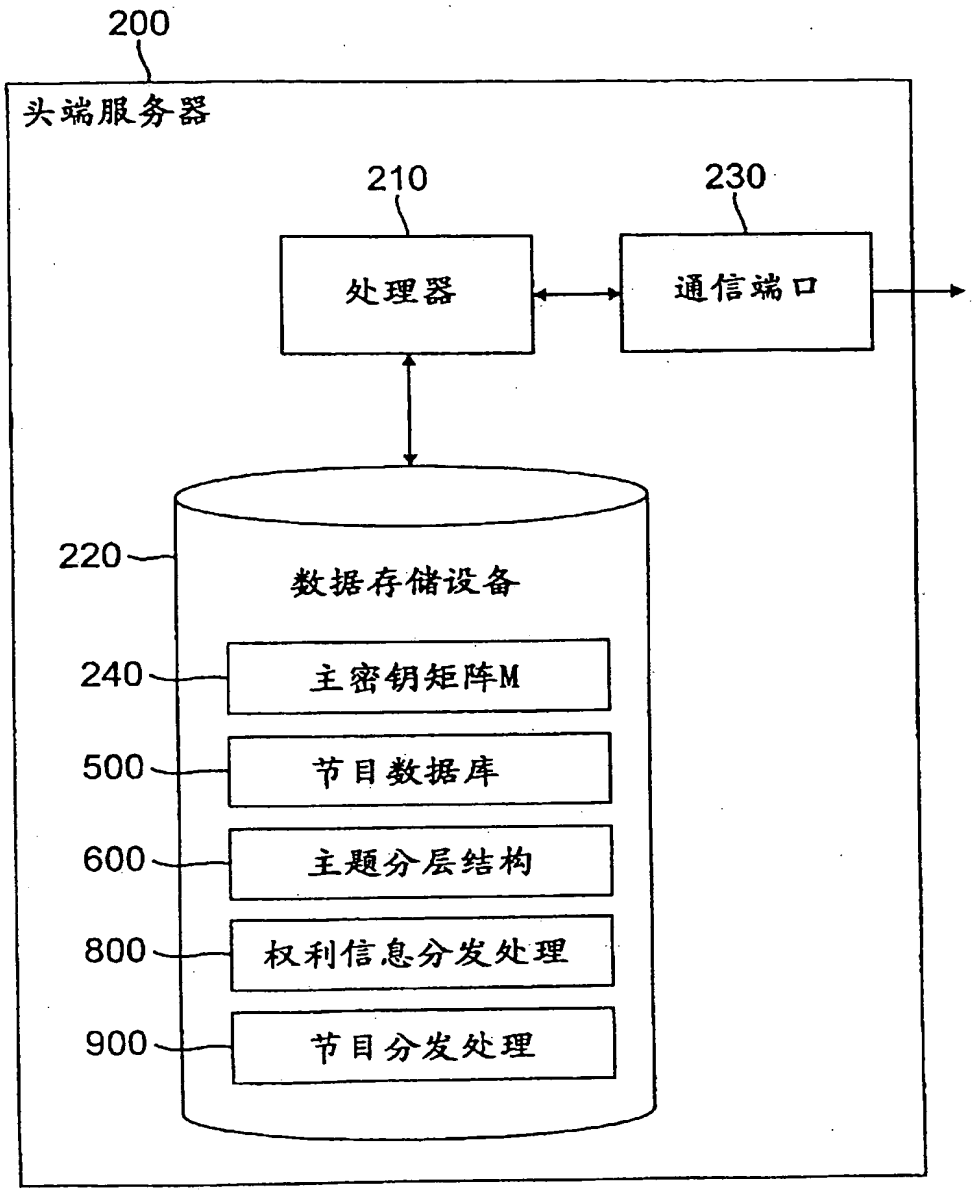

200
头端服务器
210
处理器
230
通信端口
220
数据存储设备
240
主密钥矩阵M
500
节目数据库
600
主题分层结构
800
权利信息分发处理
900
节目分发处理

图 2

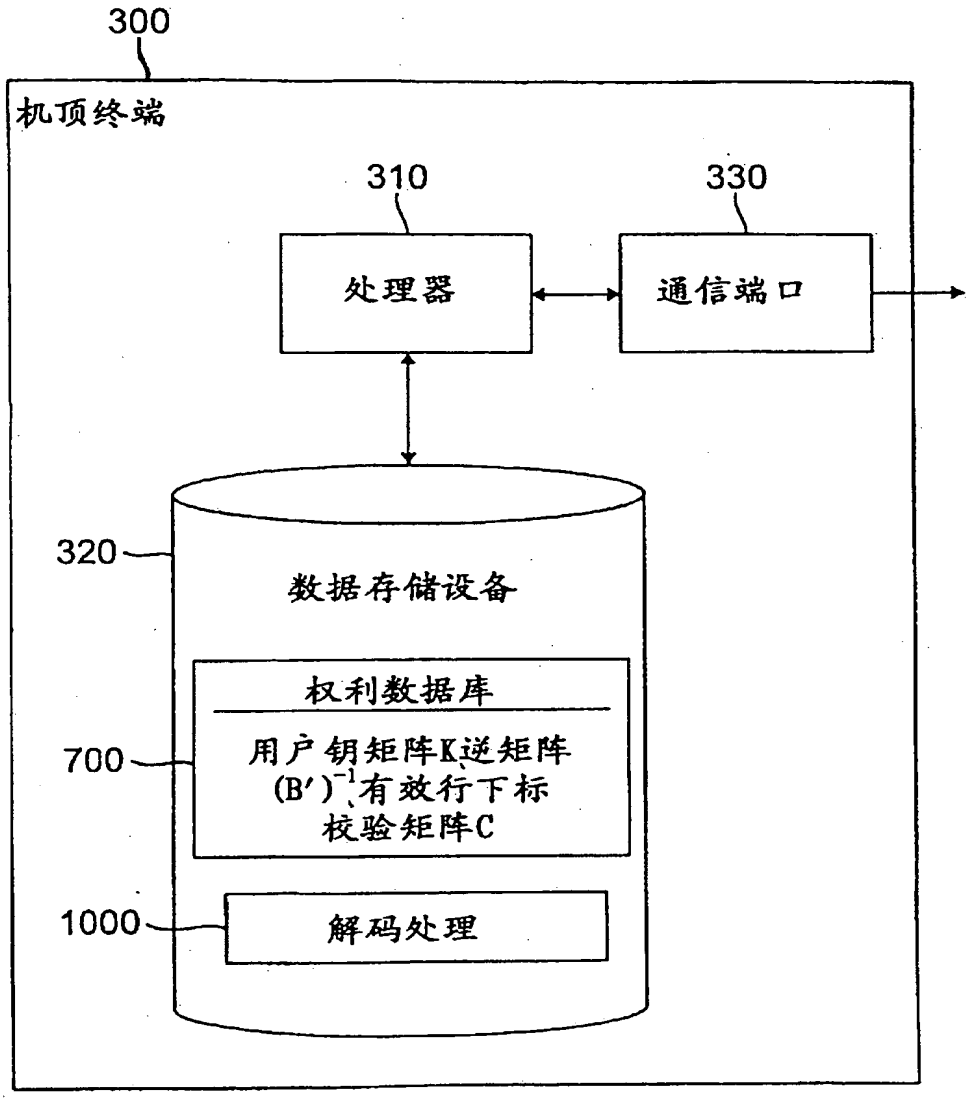

300
机顶终端
310
处理器
330
通信端口
320
数据存储设备
权利数据库
700
用户钥矩阵K逆矩阵
$(B')^{-1}$、有效行下标
校验矩阵C
1000
解码处理

图 3